

Zuzanna Jordan¹, Wojciech Kołakowski²

https://doi.org/10.29316/9788368103359_13

PRAWNA ODPOWIEDZIALNOŚĆ PODMIOTÓW ZA NARUSZENIA CYBERBEZPIECZEŃSTWA

LEGAL LIABILITY OF ENTITIES FOR CYBERSECURITY BREACHES

Streszczenie

Rozwój technologii cyfrowych oraz powszechne wykorzystanie systemów teleinformatycznych przez podmioty publiczne i prywatne spowodowały wzrost znaczenia cyberbezpieczeństwa jako przedmiotu regulacji prawnej. Opracowanie podejmuje analizę prawnej odpowiedzialności podmiotów za naruszenia cyberbezpieczeństwa, ze szczególnym uwzględnieniem normatywnych podstaw tej odpowiedzialności oraz jej zróżnicowanego charakteru. Omówiono obowiązki prawne wynikające z przepisów prawa krajowego i unijnego, w tym dyrektywy NIS 2 oraz ustawy o krajowym systemie cyberbezpieczeństwa. Przedstawiono również skutki prawne naruszeń cyberbezpieczeństwa oraz formy odpowiedzialności administracyjnej, cywilnoprawnej i karnej. Celem opracowania jest wykazanie, że naruszenia cyberbezpieczeństwa stanowią zdarzenia prawnie relewantne, rodzące wielopoziomowe

¹ <https://orcid.org/0009-0009-2636-8501>, email: zuzanna.jordan@protonmail.com

² <https://orcid.org/0009-0009-3300-1580>, email: wgkkołakowski@gmail.com

konsekwencje prawne. W opracowaniu zastosowano metodę analizy dogmatyczno-prawnej, polegającą na badaniu treści obowiązujących aktów normatywnych regulujących cyberbezpieczeństwo oraz odpowiedzialność prawną za naruszenia obowiązków w tym zakresie. Analizie poddano w szczególności przepisy prawa Unii Europejskiej oraz prawa krajowego odnoszące się do funkcjonowania krajowego systemu cyberbezpieczeństwa. Uzupełniając wykorzystano analizę piśmiennictwa prawniczego, w zakresie istotnym dla określenia charakteru i zakresu odpowiedzialności prawnej za naruszenia cyberbezpieczeństwa

Słowa kluczowe: cyberbezpieczeństwo, odpowiedzialność prawna, naruszenie cyberbezpieczeństwa, systemy teleinformatyczne, prawo cyberbezpieczeństwa

Abstract

The development of digital technologies and the widespread use of ICT systems by public and private entities have resulted in an increase in the importance of cybersecurity as a subject of legal regulation. The study provides an analysis of the legal liability of entities for cybersecurity breaches, with particular emphasis on the normative bases of this liability and its diverse nature. Legal obligations arising from the provisions of national and EU law, including the NIS 2 Directive and the Act on the National Cybersecurity System, are discussed. The legal consequences of cybersecurity breaches and forms of administrative, civil and criminal liability are also presented. The aim of the study is to demonstrate that cybersecurity breaches are legally relevant events that have multi-level legal consequences. The study uses the method of dogmatic and legal analysis, which consists in examining the content of the applicable normative acts regulating cybersecurity and legal liability for breaches of obligations in this regard. In particular, the provisions of European Union law and national law relating to the functioning of the national cybersecurity system were analysed. In addition, the analysis of legal literature was used to the extent relevant to determining the nature and scope of legal liability for cybersecurity breaches.

Keywords: cybersecurity, legal liability, cybersecurity breach, ICT systems, cybersecurity law

Wstęp

Postępująca cyfryzacja życia społecznego i gospodarczego sprawiła, że systemy teleinformatyczne stały się podstawowym narzędziem realizacji

zadań publicznych oraz prowadzenia działalności gospodarczej. Przetwarzanie informacji, świadczenie usług oraz komunikacja coraz częściej odbywają się w cyberprzestrzeni, co zwiększa znaczenie zagadnień związanych z bezpieczeństwem funkcjonowania systemów informacyjnych. Jednocześnie rozwój technologiczny wiąże się z narastającą liczbą zagrożeń, które mogą prowadzić do naruszeń cyberbezpieczeństwa.

Cyberbezpieczeństwo zostało ujęte w obowiązujących regulacjach prawnych jako przedmiot ochrony wymagający podejmowania określonych działań prewencyjnych oraz reakcyjnych. Ustawodawca unijny oraz krajowy nałożył na wybrane podmioty obowiązki zapewnienia odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych, w tym w szczególności obowiązki w zakresie zarządzania ryzykiem oraz zdolności do zapobiegania incydentom i reagowania na nie (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 21-23). Naruszenie tych obowiązków może skutkować powstaniem odpowiedzialności prawnej, niezależnie od tego, czy do naruszenia doszło na skutek działania, czy zaniechania podmiotu zobowiązanego.

Warto zauważyć, że cyberbezpieczeństwo nie jest już postrzegane wyłącznie jako zagadnienie techniczne (Chiara, 2024, s. 2-3). Obowiązujące regulacje prawne nadają mu charakter normatywny, czyniąc z niego element porządku prawnego podlegający ocenie z punktu widzenia zgodności zachowania podmiotów z prawem. Naruszenia cyberbezpieczeństwa mogą prowadzić do zakłócenia ciągłości działania usług, naruszenia praw osób fizycznych, a w określonych przypadkach również do zagrożenia interesu publicznego (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2, art. 8).

Celem niniejszego opracowania jest analiza prawnej odpowiedzialności podmiotów za naruszenia cyberbezpieczeństwa. Opracowanie koncentruje się na identyfikacji obowiązków prawnych związanych z zapewnieniem cyberbezpieczeństwa oraz na omówieniu konsekwencji prawnych wynikających z ich naruszenia. W opracowaniu zastosowano metodę analizy dogmatycznoprawnej, polegającą na badaniu treści obowiązujących aktów normatywnych regulujących zagadnienia cyberbezpieczeństwa.

Cyberbezpieczeństwo jako przedmiot ochrony prawnej i źródło obowiązków

Pojęcie cyberbezpieczeństwa nie posiada jednolitego, uniwersalnego znaczenia funkcjonującego we wszystkich porządkach prawnych. Jego treść normatywna jest kształtowana przez akty prawa krajowego oraz unijnego, które ujmują cyberbezpieczeństwo jako przedmiot ochrony prawnej wymagający podejmowania określonych działań organizacyjnych i technicznych. W tym ujęciu cyberbezpieczeństwo stanowi element bezpieczeństwa państwa, bezpieczeństwa informacji oraz bezpieczeństwa obrotu gospodarczego. Na gruncie prawa krajowego definicja cyberbezpieczeństwa została zawarta w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zgodnie z art. 2 pkt 4 tej ustawy cyberbezpieczeństwo oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz usług z nimi powiązanych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 4). Definicja ta wskazuje jednoznacznie, że cyberbezpieczeństwo nie ogranicza się wyłącznie do ochrony danych jako takich, lecz obejmuje również ciągłość i prawidłowość funkcjonowania systemów oraz usług opartych na technologiach informacyjnych. Ujęcie normatywne cyberbezpieczeństwa akcentuje jego charakter funkcjonalny. Nie jest ono rozumiane jako stan absolutnego bezpieczeństwa, lecz jako zdolność systemów informacyjnych do przeciwstawiania się zagrożeniom oraz do reagowania na incydenty. Tym samym cyberbezpieczeństwo przyjmuje postać dynamicznego procesu, którego celem jest ograniczanie ryzyka naruszeń oraz minimalizowanie ich skutków prawnych i faktycznych (Terebiński, 2018, s. 216-218).

Podobne podejście zostało przyjęte na poziomie prawa Unii Europejskiej. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (tzw. dyrektywa NIS 2) posługuje się pojęciem cyberbezpieczeństwa w kontekście bezpieczeństwa sieci i systemów informatycznych, kładąc nacisk na obowiązek zapewnienia wysokiego wspólnego poziomu ochrony w całej Unii (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022) (Chronowska-Sioła, 2025, s. 15-16) (Skoczylas, 2025, s. 231-233). Regulacja ta traktuje cyberbezpieczeństwo jako wartość podlegającą ochronie prawnej ze względu na znaczenie systemów informacyjnych dla funkcjonowania gospodarki, administracji publicznej oraz społeczeństwa. Normatywne

ujęcie cyberbezpieczeństwa prowadzi do wniosku, że jego zapewnienie nie ma charakteru fakultatywnego. Obowiązujące przepisy prawa nakładają na określone podmioty konkretne obowiązki, których celem jest utrzymanie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych. Naruszenie tych obowiązków skutkuje powstaniem konsekwencji prawnych, niezależnie od tego, czy doszło do rzeczywistej szkody. Cyberbezpieczeństwo funkcjonuje zatem w porządku prawnym jako przedmiot regulacji o charakterze prewencyjnym, a jednocześnie jako podstawa odpowiedzialności prawnej w przypadku wystąpienia naruszeń.

Cyberbezpieczeństwo, ujmowane w perspektywie normatywnej, pozostaje w ścisłym związku z pojęciem bezpieczeństwa prawnego oraz ochroną interesu publicznego. Funkcjonowanie współczesnych państw i gospodarek opiera się w znacznym stopniu na niezawodności systemów teleinformatycznych, które służą realizacji zadań publicznych, świadczeniu usług kluczowych oraz przetwarzaniu informacji o istotnym znaczeniu społecznym. Zakłócenia w tym obszarze mogą prowadzić do naruszenia stabilności porządku prawnego oraz osłabienia zaufania do instytucji publicznych i prywatnych. Bezpieczeństwo prawne rozumiane jest w doktrynie jako stan, w którym adresaci norm prawnych mogą racjonalnie przewidywać skutki swoich działań oraz polegać na stabilnym i skutecznym funkcjonowaniu systemu prawa (Chałubińska-Jentkiewicz, 2022, s. 23-25). Naruszenia cyberbezpieczeństwa, polegające przykładowo na zakłóceniu działania systemów administracji publicznej lub infrastruktury informacyjnej, mogą prowadzić do sytuacji, w których realizacja praw i obowiązków wynikających z przepisów prawa staje się utrudniona lub niemożliwa. W tym ujęciu cyberbezpieczeństwo stanowi warunek faktyczny skuteczności obowiązujących norm prawnych. Z perspektywy interesu publicznego cyberbezpieczeństwo pełni funkcję ochronną wobec wartości o fundamentalnym znaczeniu, takich jak bezpieczeństwo państwa, porządek publiczny czy ochrona praw obywateli.

Ustawodawca krajowy, wprowadzając regulacje dotyczące krajowego systemu cyberbezpieczeństwa, wskazuje wprost na konieczność zapewnienia nieprzerwanego i bezpiecznego świadczenia usług kluczowych oraz cyfrowych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 1 ust. 1, art. 3). Oznacza to, że cyberbezpieczeństwo nie jest wyłącznie interesem indywidualnym podmiotów eksploatujących systemy informacyjne, lecz stanowi dobro o charakterze publicznym. Również prawo

Unii Europejskiej traktuje cyberbezpieczeństwo jako element wspólnego interesu państw członkowskich. Celem regulacji unijnych jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, co uzasadnione jest transgranicznym charakterem zagrożeń występujących w cyberprzestrzeni (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, motyw 1, art. 1). Ataki cybernetyczne rzadko ograniczają się do terytorium jednego państwa, a ich skutki mogą oddziaływać na funkcjonowanie rynku wewnętrznego oraz bezpieczeństwo obywateli Unii (Chałubińska-Jentkiewicz, 2022, s. 24-25). Uznanie cyberbezpieczeństwa za element interesu publicznego uzasadnia ingerencję ustawodawcy w sferę działalności podmiotów publicznych i prywatnych poprzez nałożenie na nie określonych obowiązków. Obowiązki te mają charakter prewencyjny i służą ograniczeniu ryzyka wystąpienia incydentów, a jednocześnie stanowią podstawę do przypisania odpowiedzialności prawnej w przypadku ich naruszenia. W konsekwencji cyberbezpieczeństwo funkcjonuje w porządku prawnym jako wartość chroniona, której naruszenie może prowadzić do negatywnych konsekwencji nie tylko dla danego podmiotu, lecz także dla szeroko rozumianego interesu publicznego.

Ujęcie cyberbezpieczeństwa jako elementu bezpieczeństwa prawnego oraz interesu publicznego prowadzi do konieczności jego normatywnego zabezpieczenia poprzez nałożenie na określone podmioty konkretnych obowiązków prawnych. Obowiązki te nie mają charakteru wyłącznie deklaratywnego, lecz stanowią normatywnie określone powinności, których realizacja podlega ocenie z punktu widzenia legalności zachowania adresatów norm prawnych. Na gruncie prawa krajowego podstawowym aktem regulującym obowiązki w zakresie cyberbezpieczeństwa jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustawodawca wskazuje w niej kategorie podmiotów zobowiązanych do zapewnienia bezpieczeństwa systemów informacyjnych, w szczególności operatorów usług kluczowych oraz dostawców usług cyfrowych. Nałożone na te podmioty obowiązki obejmują m.in. podejmowanie działań zapobiegających incydentom, zapewnienie zdolności do wykrywania zagrożeń oraz reagowania na naruszenia cyberbezpieczeństwa (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 8 ust. 1-3, art. 11) (Chronowska-Sioła, 2025, s. 18-19) (Szpor, 2019, s. 42-45). Charakterystyczną cechą obowiązków w zakresie cyberbezpieczeństwa jest ich prewencyjny charakter. Prawo

nie ogranicza się bowiem do reakcji na skutki incydentów, lecz zobowiązuje podmioty do podejmowania działań z wyprzedzeniem, w szczególności poprzez zarządzanie ryzykiem związanym z funkcjonowaniem systemów informacyjnych. Oznacza to, że odpowiedzialność prawna może powstać również w sytuacji, gdy do naruszenia doszło na skutek niewystarczających działań zapobiegawczych, a nie bezpośredniego naruszenia przepisów o charakterze technicznym. Podobne podejście przyjęto w prawie Unii Europejskiej. Dyrektywa NIS 2 rozszerza krąg podmiotów objętych regulacją oraz wzmacnia obowiązki związane z zarządzaniem cyberbezpieczeństwem, kładąc nacisk na odpowiedzialność organizacyjną i systemową. Regulacja ta zakłada, że zapewnienie cyberbezpieczeństwa stanowi element należytej staranności podmiotów objętych jej zakresem, a niedopełnienie wynikających z niej obowiązków może prowadzić do zastosowania środków nadzorczych oraz sankcji (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 20-23). Istotne znaczenie ma również fakt, że obowiązki w zakresie cyberbezpieczeństwa mają charakter ciągły. Nie ograniczają się one do jednorazowego wdrożenia określonych rozwiązań, lecz wymagają stałego monitorowania zagrożeń, aktualizacji środków ochrony oraz dostosowywania procedur do zmieniającego się środowiska teleinformatycznego. W konsekwencji naruszenie cyberbezpieczeństwa może wynikać zarówno z braku reakcji na incydent, jak i z zaniechania aktualizacji lub utrzymania odpowiedniego poziomu zabezpieczeń. Ukształtowanie cyberbezpieczeństwa jako przedmiotu obowiązków prawnych stanowi podstawę do dalszej analizy odpowiedzialności prawnej podmiotów. Skoro bowiem ustawodawca nakłada na określone podmioty konkretne powinności, to ich niewykonanie lub nienależyte wykonanie otwiera drogę do przypisania odpowiedzialności, niezależnie od tego, czy naruszenie miało charakter zawiniony. Tym samym cyberbezpieczeństwo funkcjonuje w porządku prawnym jako obszar normalnie zorganizowany, w którym obowiązki i odpowiedzialność pozostają ze sobą w ścisłym związku.

Naruszenie cyberbezpieczeństwa jako zdarzenie prawnie relewantne

Analiza odpowiedzialności prawnej podmiotów za naruszenia cyberbezpieczeństwa wymaga w pierwszej kolejności ustalenia, czym w sensie

normatywnym jest samo naruszenie cyberbezpieczeństwa. Pojęcie to nie ma charakteru potocznego ani technicznego, lecz zostało ukształtowane przez przepisy prawa, które nadają mu określone znaczenie prawne i wiążą z nim konkretne konsekwencje normatywne. Na gruncie prawa krajowego kluczowe znaczenie ma definicja incydentu zawarta w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Zgodnie z art. 2 pkt 5 tej ustawy incydent oznacza zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Definicja ta ma charakter szeroki i obejmuje zarówno zdarzenia, które już spowodowały zakłócenia w funkcjonowaniu systemów informacyjnych, jak i takie, które potencjalnie mogą do nich doprowadzić (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 5) (Skoczylas, 2025, s. 233-234). Powyższe ujęcie wskazuje, że naruszenie cyberbezpieczeństwa nie jest ograniczone wyłącznie do sytuacji wystąpienia realnej szkody. Już samo wystąpienie zdarzenia stwarzającego zagrożenie dla poufności, integralności, dostępności lub autentyczności danych bądź usług może zostać zakwalifikowane jako incydent w rozumieniu przepisów prawa. Tym samym ustawodawca przyjmuje prewencyjny model ochrony cyberbezpieczeństwa, w którym znaczenie prawne mają również zdarzenia o charakterze potencjalnym. Prawo unijne posługuje się zbliżoną konstrukcją pojęciową. Dyrektywa NIS 2 definiuje incydent jako zdarzenie zagrażające dostępności, autentyczności, integralności lub poufności przechowywanych, przesyłanych lub przetwarzanych danych albo usług oferowanych przez sieci i systemy informatyczne. Regulacja ta kładzie nacisk na skutki zdarzenia dla funkcjonowania usług oraz na jego wpływ na bezpieczeństwo systemów informacyjnych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 6 pkt 6). Istotnym elementem normatywnego rozumienia naruszenia cyberbezpieczeństwa jest jego oderwanie od winy podmiotu zobowiązanego. Przepisy prawa nie uzależniają kwalifikacji danego zdarzenia jako naruszenia od zawinionego działania lub zaniechania. Oznacza to, że naruszenie cyberbezpieczeństwa może wystąpić również w sytuacji, gdy podmiot dochował należytej staranności, lecz mimo to doszło do incydentu. Kwestia winy nabiera znaczenia dopiero na etapie oceny odpowiedzialności prawnej. Naruszenie cyberbezpieczeństwa pełni zatem w porządku prawnym funkcję zdarzenia prawnie relewantnego, które uruchamia określone obowiązki po stronie podmiotów zobowiązanych, w szczególności obowiązki zgłoszeniowe, informacyjne oraz

naprawcze. Jednocześnie stanowi ono punkt wyjścia do oceny, czy doszło do naruszenia obowiązków prawnych w zakresie zapewnienia cyberbezpieczeństwa, a w konsekwencji – do przypisania odpowiedzialności prawnej.

Naruszenia cyberbezpieczeństwa nie stanowią jednorodnej kategorii zdarzeń. Obowiązujące regulacje prawne różnicują je ze względu na skalę, skutki oraz znaczenie dla funkcjonowania systemów informacyjnych i świadczonych usług. Zróżnicowanie to ma istotne znaczenie prawne, ponieważ determinuje zakres obowiązków podmiotów zobowiązanych oraz możliwe konsekwencje prawne związane z wystąpieniem danego naruszenia. Na gruncie prawa krajowego ustawodawca posługuje się kategorią incydentów, wprowadzając jednocześnie ich gradację. Ustawa o krajowym systemie cyberbezpieczeństwa wyróżnia m.in. incydenty poważne oraz incydenty krytyczne, których wystąpienie wiąże się ze zwiększonym poziomem zagrożenia dla ciągłości działania usług kluczowych lub systemów informacyjnych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 2 pkt 6-8, art. 12). Kryteria kwalifikacji danego zdarzenia do określonej kategorii incydentów obejmują w szczególności liczbę użytkowników dotkniętych skutkami zdarzenia, czas trwania zakłócenia oraz jego wpływ na bezpieczeństwo publiczne lub porządek publiczny. Powyższa klasyfikacja pełni funkcję normatywną, a nie wyłącznie opisową. Zakwalifikowanie naruszenia jako incydentu o określonym charakterze rodzi po stronie podmiotów zobowiązanych konkretne obowiązki prawne, w tym obowiązki niezwłocznego zgłoszenia zdarzenia właściwym organom oraz podjęcia działań zmierzających do ograniczenia jego skutków. Im wyższy stopień zagrożenia związany z naruszeniem cyberbezpieczeństwa, tym szerszy zakres ingerencji organów publicznych oraz intensywniejsze środki nadzorcze. Również prawo Unii Europejskiej przyjmuje zróżnicowane podejście do naruszeń cyberbezpieczeństwa. Dyrektywa NIS 2 posługuje się pojęciem incydentu znaczącego, którego kwalifikacja uzależniona jest od wpływu zdarzenia na świadczenie usług, zakresu oddziaływania oraz potencjalnych skutków transgranicznych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 6 pkt 7, art. 23). Ujęcie to podkreśla funkcjonalny charakter naruszeń cyberbezpieczeństwa, koncentrując się nie tyle na przyczynie zdarzenia, ile na jego skutkach dla systemów i użytkowników. Znaczenie prawne rozróżnienia poszczególnych rodzajów naruszeń cyberbezpieczeństwa polega również na tym, że wpływa ono na zakres

odpowiedzialności prawnej podmiotów. Nie każde naruszenie prowadzi automatycznie do zastosowania sankcji, jednak każde może stanowić podstawę do oceny czy podmiot wywiązał się z nałożonych na niego obowiązków w zakresie zapewnienia cyberbezpieczeństwa. W przypadku incydentów o większej wadze ustawodawca przewiduje dalej idące konsekwencje, w tym możliwość nałożenia kar administracyjnych lub zastosowania środków nadzorczych. W konsekwencji rodzaje naruszeń cyberbezpieczeństwa należy postrzegać jako element systemu oceny prawnej zachowania podmiotów zobowiązanych. Klasyfikacja ta pozwala na proporcjonalne reagowanie na zagrożenia, z jednej strony zapewniając ochronę interesu publicznego, z drugiej zaś uwzględniając stopień ryzyka oraz faktyczne skutki danego zdarzenia. Stanowi to istotne ogniwo łączące pojęcie naruszenia cyberbezpieczeństwa z mechanizmami odpowiedzialności prawnej.

Wystąpienie naruszenia cyberbezpieczeństwa nie pozostaje bez znaczenia w sferze prawnej. Przepisy prawa wiążą z takim zdarzeniem określone skutki normatywne, które aktualizują się niezależnie od dalszej oceny odpowiedzialności podmiotu zobowiązanego. Naruszenie cyberbezpieczeństwa stanowi bowiem zdarzenie prawnie relewantne, uruchamiające po stronie podmiotów objętych regulacją szereg obowiązków o charakterze publicznoprawnym. Na gruncie prawa krajowego podstawowym skutkiem prawnym naruszenia cyberbezpieczeństwa jest powstanie obowiązku podjęcia działań zmierzających do obsługi incydentu. Ustawa o krajowym systemie cyberbezpieczeństwa nakłada na podmioty zobowiązane obowiązek niezwłocznego wykrywania, rejestrowania oraz obsługi incydentów, w tym podejmowania działań naprawczych i zapobiegawczych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 8 ust. 1 pkt 1-3, art. 11 ust. 1). Obowiązki te mają charakter bezwzględny i aktualizują się z chwilą wystąpienia zdarzenia spełniającego ustawowe kryteria incydentu. Kolejnym istotnym skutkiem prawnym naruszenia cyberbezpieczeństwa jest obowiązek zgłoszeniowy. W przypadku incydentów o określonym stopniu istotności podmioty zobowiązane są do przekazania informacji właściwym organom, w szczególności zespołom reagowania na incydenty bezpieczeństwa komputerowego. Celem tego obowiązku jest umożliwienie koordynacji działań na poziomie krajowym oraz ograniczenie potencjalnych skutków naruszenia dla innych podmiotów i użytkowników systemów informacyjnych (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie

cyberbezpieczeństwa, 2018, art. 12 ust. 1-3). Naruszenie cyberbezpieczeństwa może również prowadzić do intensyfikacji nadzoru ze strony organów publicznych. W sytuacjach uzasadnionych charakterem lub skalą incydentu organy właściwe mogą podejmować działania kontrolne, wydawać zalecenia lub polecenia dotyczące sposobu usunięcia skutków naruszenia oraz zapobiegania jego powtórzeniu. Działania te mają charakter prewencyjno-naprawczy i nie stanowią jeszcze sankcji w ścisłym znaczeniu tego słowa. Warto podkreślić, że skutki prawne naruszenia cyberbezpieczeństwa mają charakter autonomiczny względem odpowiedzialności prawnej. Oznacza to, że samo wystąpienie naruszenia rodzi określone obowiązki, niezależnie od tego, czy w dalszym etapie zostanie stwierdzone naruszenie przepisów skutkujące nałożeniem sankcji. Innymi słowy, obowiązki reakcyjne i zgłoszeniowe pełnią funkcję zabezpieczającą interes publiczny, a nie represyjną. Analogiczne rozwiązania przyjęto na poziomie prawa Unii Europejskiej. Dyrektywa NIS 2 przewiduje obowiązki zgłaszania incydentów w określonych terminach oraz obowiązek przekazywania informacji umożliwiających ocenę skutków naruszenia dla świadczenia usług (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 23). Regulacja ta wzmacnia znaczenie reakcji na incydent jako elementu systemu cyberbezpieczeństwa, traktując naruszenie nie tylko jako problem podmiotu, którego dotyczy, lecz jako potencjalne zagrożenie o szerszym oddziaływaniu. Skutki prawne naruszenia cyberbezpieczeństwa stanowią zatem istotne ogniwo pomiędzy samym zdarzeniem a oceną odpowiedzialności prawnej podmiotu. To właśnie na tym etapie możliwe jest ustalenie czy podmiot dochował obowiązków w zakresie reagowania na incydent, co w dalszej kolejności może mieć decydujące znaczenie dla przypisania odpowiedzialności administracyjnej, cywilnej lub innej formy odpowiedzialności prawnej.

Formy odpowiedzialności prawnej za naruszenia cyberbezpieczeństwa

Odpowiedzialność administracyjnoprawna stanowi podstawowy i najczęściej stosowany mechanizm reakcji państwa na naruszenia cyberbezpieczeństwa. Jej celem nie jest represja sensu stricto, lecz zapewnienie skutecznego wykonywania obowiązków nałożonych na podmioty zobowiązane oraz ochrona interesu publicznego poprzez zapobieganie dalszym naruszeniom.

Odpowiedzialność ta realizowana jest w ramach stosunków administracyjnoprawnych, z udziałem organów właściwych do spraw cyberbezpieczeństwa. Na gruncie prawa krajowego odpowiedzialność administracyjnoprawna za naruszenia cyberbezpieczeństwa została ukształtowana przede wszystkim w ustawie o krajowym systemie cyberbezpieczeństwa. Ustawa ta przewiduje możliwość nałożenia na podmioty zobowiązane administracyjnych kar pieniężnych w przypadku niewykonania lub nienależytego wykonania obowiązków określonych w jej przepisach (Cătană, 2025, s. 37-39). Sankcje te mają charakter publicznoprawny i są nakładane w drodze decyzji administracyjnej przez właściwy organ (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 73-75). Charakterystyczną cechą odpowiedzialności administracyjnoprawnej w obszarze cyberbezpieczeństwa jest jej w znacznym stopniu obiektywny charakter. Ustawodawca nie uzależnia możliwości nałożenia kary administracyjnej wyłącznie od wykazania winy podmiotu, lecz od stwierdzenia naruszenia obowiązków ustawowych. Oznacza to, że kluczowe znaczenie ma ocena zgodności zachowania podmiotu z nałożonymi na niego obowiązkami, a nie subiektywne nastawienie czy intencja działania. W ramach odpowiedzialności administracyjnoprawnej istotną rolę odgrywa zasada proporcjonalności (Cătană, 2025, s. 45-47).

Organ nakładający karę powinien uwzględnić charakter, wagę i czas trwania naruszenia, a także jego skutki dla bezpieczeństwa systemów informacyjnych i interesu publicznego. Ustawa przewiduje możliwość miarkowania wysokości kary administracyjnej, co pozwala na dostosowanie reakcji organu do stopnia zagrożenia wywołanego naruszeniem cyberbezpieczeństwa (Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 2018, art. 76). Odpowiedzialność administracyjnoprawna może być również poprzedzona lub uzupełniona środkami o charakterze nadzorczym. Organy właściwe są uprawnione do wydawania zaleceń, żądania usunięcia stwierdzonych nieprawidłowości oraz podejmowania innych działań zmierzających do przywrócenia zgodności z prawem. Dopiero w przypadku braku realizacji tych obowiązków lub poważnego naruszenia przepisów możliwe jest sięgnięcie po sankcje finansowe. Podobne rozwiązania zostały przyjęte na poziomie prawa Unii Europejskiej. Dyrektywa NIS 2 przewiduje obowiązek ustanowienia przez państwa członkowskie skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych za naruszenia

obowiązków w zakresie cyberbezpieczeństwa. Regulacja ta wzmacnia rolę odpowiedzialności administracyjnoprawnej jako podstawowego instrumentu egzekwowania norm dotyczących bezpieczeństwa sieci i systemów informatycznych (Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555, 2022, art. 34). W konsekwencji odpowiedzialność administracyjnoprawna pełni kluczową funkcję w systemie ochrony cyberbezpieczeństwa. Stanowi ona mechanizm zapewniający realną skuteczność norm prawnych poprzez możliwość zastosowania bezpośrednich środków władczych wobec podmiotów naruszających obowiązki ustawowe. Jednocześnie jej prewencyjny charakter sprawia, że ma ona na celu nie tylko reagowanie na naruszenia, lecz także zapobieganie ich występowaniu w przyszłości.

Obok odpowiedzialności administracyjnoprawnej naruszenia cyberbezpieczeństwa mogą rodzić również odpowiedzialność cywilnoprawną. Ma ona odmienny charakter i funkcję, gdyż jej celem jest przede wszystkim ochrona interesów prywatnych podmiotów, które poniosły szkodę w wyniku naruszenia, a także kompensacja doznanych strat. Odpowiedzialność cywilnoprawna realizowana jest w ramach stosunków prawa prywatnego i co do zasady dochodzona jest przed sądem powszechnym. Podstawą odpowiedzialności cywilnoprawnej za naruszenia cyberbezpieczeństwa są ogólne przepisy prawa cywilnego dotyczące odpowiedzialności odszkodowawczej. W zależności od okoliczności sprawy może ona przybrać postać odpowiedzialności deliktowej albo kontraktowej. W pierwszym przypadku naruszenie cyberbezpieczeństwa stanowi czyn niedozwolony, w wyniku którego poszkodowany doznał szkody. W drugim – naruszenie obowiązków związanych z zapewnieniem cyberbezpieczeństwa może być traktowane jako nienależyte wykonanie zobowiązania umownego. Charakterystyczną cechą odpowiedzialności cywilnoprawnej w omawianym obszarze jest konieczność wykazania przesłanek odpowiedzialności, w szczególności powstania szkody, bezprawności zachowania, związku przyczynowego oraz – co do zasady – winy podmiotu odpowiedzialnego. Naruszenie cyberbezpieczeństwa samo w sobie nie przesądza jeszcze o odpowiedzialności cywilnej, lecz może stanowić zdarzenie wywołujące szkodę lub zwiększające ryzyko jej wystąpienia. Szkody wynikające z naruszeń cyberbezpieczeństwa mogą mieć zarówno charakter majątkowy, jak i niemajątkowy. Do szkód majątkowych zaliczyć można m.in. straty finansowe spowodowane przerwą w działalności, utratą danych lub koniecznością przywrócenia systemów informatycznych

do prawidłowego funkcjonowania. Szkody niemajątkowe mogą natomiast dotyczyć naruszenia dóbr osobistych, takich jak prywatność czy dobre imię, zwłaszcza w sytuacjach związanych z nieuprawnionym ujawnieniem informacji. Istotnym zagadnieniem w kontekście odpowiedzialności cywilnoprawnej jest relacja pomiędzy obowiązkami publicznoprawnymi a standardem należytej staranności wymaganym w stosunkach prywatnoprawnych. Obowiązki nałożone na podmioty w przepisach dotyczących cyberbezpieczeństwa mogą pełnić funkcję punktu odniesienia przy ocenie, czy dany podmiot dochował należytej staranności. Ich naruszenie może zatem pośrednio wpływać na ocenę bezprawności lub winy w postępowaniu cywilnym. Odpowiedzialność cywilnoprawna za naruszenia cyberbezpieczeństwa pełni funkcję uzupełniającą wobec odpowiedzialności administracyjnoprawnej. Podczas gdy sankcje administracyjne służą ochronie interesu publicznego, odpowiedzialność cywilna koncentruje się na naprawieniu szkody wyrządzonej konkretnemu podmiotowi. Obie formy odpowiedzialności mogą funkcjonować równolegle, gdyż realizują odmienne cele i oparte są na różnych podstawach prawnych.

Odpowiedzialność karna za naruszenia cyberbezpieczeństwa stanowi najbardziej represyjną formę reakcji prawnej na zachowania zagrażające bezpieczeństwu systemów informacyjnych. Jej zastosowanie ograniczone jest do przypadków, w których naruszenie cyberbezpieczeństwa przybiera postać czynu zabronionego określonego w przepisach prawa karnego. Z tego względu odpowiedzialność karna pełni w systemie ochrony cyberbezpieczeństwa funkcję subsydiarną wobec odpowiedzialności administracyjnoprawnej i cywilnoprawnej. Na gruncie prawa krajowego podstawowe typy czynów zabronionych związanych z naruszeniami cyberbezpieczeństwa zostały uregulowane w Kodeksie karnym. Przepisy te penalizują m.in. nieuprawnione uzyskanie dostępu do informacji, zakłócanie pracy systemów informatycznych, niszczenie lub modyfikowanie danych oraz ingerencję w funkcjonowanie sieci teleinformatycznych (Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, 1997, art. 267-269b). Odpowiedzialność karna w tym zakresie ma na celu ochronę poufności, integralności i dostępności informacji, a także stabilności systemów informacyjnych. Charakterystyczną cechą odpowiedzialności karnej jest jej ściśle powiązanie z zasadą winy. Przypisanie odpowiedzialności karnej wymaga wykazania, że sprawca działał umyślnie albo – w przypadkach przewidzianych przez ustawę – nieumyślnie.

Sam fakt wystąpienia naruszenia cyberbezpieczeństwa nie przesądza zatem o odpowiedzialności karnej określonego podmiotu. Konieczne jest ustalenie, że zachowanie sprawcy wypełnia znamiona konkretnego typu czynu zabronionego. W kontekście odpowiedzialności karnej istotne znaczenie ma również rozróżnienie pomiędzy sprawcą bezpośredniego ataku a podmiotem zobowiązanym do zapewnienia cyberbezpieczeństwa. Odpowiedzialność karna dotyczy co do zasady osób fizycznych, które dopuściły się czynu zabronionego, a nie podmiotów jako takich. Tym samym brak zapewnienia odpowiedniego poziomu cyberbezpieczeństwa przez organizację nie prowadzi automatycznie do odpowiedzialności karnej, chyba że możliwe jest przypisanie konkretnej osobie fizycznej zachowania wypełniającego znamiona przestępstwa. Należy również podkreślić, że odpowiedzialność karna nie służy egzekwowaniu obowiązków o charakterze prewencyjnym. Jej funkcją jest reagowanie na najpoważniejsze naruszenia cyberbezpieczeństwa, które godzą w podstawowe dobra prawne, takie jak bezpieczeństwo informacji, porządek publiczny czy interesy majątkowe. Z tego względu prawo karne pełni rolę środka ostatecznego, stosowanego w sytuacjach, w których inne formy odpowiedzialności okazują się niewystarczające. W systemie ochrony cyberbezpieczeństwa odpowiedzialność karna stanowi zatem element uzupełniający, skoncentrowany na zwalczaniu najcięższych form naruszeń. Jej znaczenie polega przede wszystkim na funkcji odstraszałej oraz ochronie podstawowych wartości, podczas gdy zasadniczy ciężar zapewnienia cyberbezpieczeństwa oraz reagowania na incydenty spoczywa na instrumentach administracyjnoprawnych i organizacyjnych.

Podsumowanie

Przeprowadzona analiza prowadzi do wniosku, że cyberbezpieczeństwo stanowi obecnie istotny przedmiot regulacji prawnej, a jego naruszenie nie jest wyłącznie problemem technicznym, lecz zdarzeniem o doniosłych konsekwencjach normatywnych. Obowiązujące regulacje krajowe i unijne jednoznacznie nadają cyberbezpieczeństwu status dobra prawnie chronionego, którego ochrona służy zarówno interesom indywidualnym, jak i interesowi publicznemu. W opracowaniu wykazano, że naruszenie cyberbezpieczeństwa funkcjonuje w porządku prawnym jako zdarzenie prawnie relewantne, uruchamiające określone skutki prawne niezależnie od dalszej

oceny odpowiedzialności podmiotu zobowiązanego. Już samo wystąpienie incydentu aktualizuje obowiązki o charakterze reakcyjnym i informacyjnym, co potwierdza prewencyjny model ochrony przyjęty przez ustawodawcę. Model ten koncentruje się nie tylko na sankcjonowaniu naruszeń, lecz również na minimalizowaniu ich skutków oraz zapobieganiu eskalacji zagrożeń. Analiza form odpowiedzialności prawnej prowadzi do wniosku, że zasadniczą rolę w systemie ochrony cyberbezpieczeństwa odgrywa odpowiedzialność administracyjnoprawna. To ona stanowi podstawowy instrument egzekwowania obowiązków nałożonych na podmioty zobowiązane oraz zapewnienia skuteczności norm prawa cyberbezpieczeństwa.

Odpowiedzialność cywilnoprawna pełni natomiast funkcję kompensacyjną, chroniąc interesy podmiotów, które poniosły szkodę w wyniku naruszenia. Odpowiedzialność karna, ze względu na swój represyjny charakter i konieczność wykazania winy, ma znaczenie uzupełniające i znajduje zastosowanie jedynie w przypadku najpoważniejszych naruszeń. W świetle powyższych ustaleń należy stwierdzić, że odpowiedzialność prawna za naruszenia cyberbezpieczeństwa ma charakter wielopoziomowy i zróżnicowany, co pozwala na elastyczne i proporcjonalne reagowanie na zagrożenia występujące w cyberprzestrzeni. Jednocześnie takie ukształtowanie systemu odpowiedzialności wymaga od podmiotów objętych regulacją stałego monitorowania obowiązków prawnych oraz podejmowania działań wykraczających poza minimalne wymogi formalne. Z perspektywy *de lege ferenda* zasadne wydaje się dalsze doprecyzowywanie relacji pomiędzy obowiązkami publicznoprawnymi a standardem należytej staranności w prawie prywatnym, w szczególności w kontekście odpowiedzialności cywilnoprawnej. Ponadto istotnym kierunkiem rozwoju regulacji powinno być wzmocnienie mechanizmów prewencyjnych, w tym promowanie kultury zgodności z prawem cyberbezpieczeństwa oraz zwiększanie świadomości prawnej podmiotów zobowiązanych.

Podsumowując, cyberbezpieczeństwo należy postrzegać jako trwały i dynamiczny element współczesnego porządku prawnego. Skuteczność ochrony w tym obszarze zależy nie tylko od treści obowiązujących regulacji, lecz również od ich konsekwentnego egzekwowania oraz właściwego rozumienia odpowiedzialności prawnej jako instrumentu służącego ochronie zarówno interesu publicznego, jak i praw jednostki.

Literatura

1. Cătană, E. L. (2025). An administrative law approach of cybersecurity rules: The case of Romania in the context of EU and international law. *Studia Iuridica Lublinensia*, 34(1), 37-47.
2. Chałubińska-Jentkiewicz, K. (2022). Cyberspace as an area of legal regulation. W: K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński (red.), *Cybersecurity in Poland: Legal aspects* (s. 23-25). Springer.
3. Chiara, P. G. (2024). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review*, 53, 1-10.
4. Chronowska-Sioła, E. (2025). Unijna dyrektywa NIS 2 w obszarze cyberbezpieczeństwa – analiza podmiotów kluczowych i podmiotów ważnych. *Cybersecurity and Law*, 2(14), 15-19.
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii (NIS 2) (2022). *Dziennik Urzędowy Unii Europejskiej*, L 333, 1-137.
6. Ottis, R., Lorents, P. (2010). Cyberspace: Definition and implications. W: *Proceedings of the 5th International Conference on Information Warfare and Security* (s. 1-10). Academic Conferences Ltd.
7. Skoczylas, D. (2025). The NIS 2 Directive and the cybersecurity of public administrations. *Discourse of Law and Administration*, 1, 231-234.
8. Szpor, G. (2019). *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*. Wolters Kluwer.
9. Terebiński, B. (2018). Bezpieczeństwo teleinformatyczne jako podstawa funkcjonowania współczesnego państwa. *Obronność – Zeszyty Naukowe*, 1(25), 216-218.
10. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (2018). *Dziennik Ustaw*, poz. 1560 ze zm.
11. Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (1997). *Dziennik Ustaw*, nr 88, poz. 553 ze zm.